

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION**

UNITED STATES OF AMERICA,)	CASE NO. 1:16-cr-270
)	
PLAINTIFF,)	JUDGE SARA LIOI
)	
vs.)	
)	MEMORANDUM OPINION
LAUDEN A. SULLIVAN,)	
)	
DEFENDANT.)	

Defendant Lauden Sullivan seeks suppression of all evidence seized from his residence at 1216 West Jackson Street, Painesville, Ohio on January 22, 2016, as well as statements made by Sullivan to federal agents. (Doc. No. 13 [“Mot.”].) It is defendant’s position that a 2015 warrant issued by a magistrate judge sitting in the Eastern District of Virginia, which permitted the FBI to monitor a site devoted to the advertisement and dissemination of child pornography and deploy a Network Investigative Technique (“NIT”) to identify users who visited the website, was void (hereinafter this warrant, attached to defendant’s motion at Doc. No. 13-1, shall be referred to as the “NIT Warrant”). Because it is undisputed that the NIT Warrant led to the FBI’s discovery that Lauden had visited the website and supplied probable cause for the 2016 residential search, defendant argues that the evidence and statements must be suppressed as fruits of the poisonous tree. The government opposes the motion. (Doc. No. 16 [“Opp’n”].) On January 10, 2016, the Court conducted a hearing on the motion. At the conclusion of the hearing, the Court took the matter under advisement.

Defendant’s motion to suppress raises interesting issues relative to the interplay between recent technological advancements and the Fourth Amendment. However, the Court does not write on a clean slate. Given the fact that the underlying investigation was one of the largest sting

operations targeting a child porn website—“the Playpen” or “Website A” (as it is referred to in the supporting affidavit)—it is not surprising that dozens of district courts have already written on the enforceability of the very same Virginia warrant that is at issue in this case. The Court has the benefit of these opinions, in addition to the informative and well-written briefs supplied by the government and defendant in the present case.

The Court concludes that the initial search of defendant’s computer did not violate the Fourth Amendment, and further finds that, even if the search was unconstitutional, suppression would not be appropriate. Accordingly, and for the reasons set forth below, the Court denies defendant’s motion to suppress.

I. BACKGROUND

For a thorough understanding of the technology at issue here, including the TOR software (which is used to conceal a user’s IP address), NIT software (which is used by law enforcement to send instructions to a computer running TOR to reveal its true location), as well as the nature of the hidden or dark web (where websites like Website A operate in relative secrecy), the Court directs the reader to two prior decisions. *See United States v. Jean*, No. 5:15-CR-50087, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); *United States v. Darby*, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016).

For purposes of framing the issues presented in defendant’s motion, the Court relies on the succinct explanation supplied in a prior case from this judicial district, *United States v. Libbey-Tipton*, Case No. 1:16-CR-236, Doc. No. 19 (N.D. Ohio Oct. 19, 2016). There, the court wrote:

On or about February 20, 2015, the government obtained an order from the Eastern District of Virginia allowing it to seize control of the operation of “Website A.” Website A contains various sections and forums related to child

pornography. Website A requires users to install publically available computer software [called TOR or an “onion router”] before accessing the site. The software prevents someone attempting to monitor the internet connection from learning the user’s physical location by routing communications through other locations. In this way, law enforcement cannot ascertain through public lookups the location of the users of Website A.

Pursuant to the Virginia warrant, the government was authorized to deploy a Network Investigative Technique (“NIT”). Each time a user logged onto Website A with a username and password, the FBI deployed the NIT which sent signals to the user’s computer. Those communications were designed to cause the user’s computer to deliver information to the government that identified the actual location of the user. The information included, among other things, the user’s actual IP address.

Id. at *1-2.

Using the NIT, the FBI determined that a person going by the username of “554422” created an account on Website A on January 21, 2015, and that, on March 1, 2015, the same person logged into the website, during which he accessed several images of child pornography and still shots from a video depicting the same. Cross-referencing the IP address associated with “554422” against publically available databases, the FBI determined that the IP address was operated by the Internet Service Provider (“ISP”) Time Warner. Through a subpoena/summons issued to Time Warner on March 11, 2015, the FBI traced the IP address to a home in Painesville, Ohio, where defendant lived.

On January 19, 2016, Magistrate Judge William H. Baughman Jr., sitting in the Northern District of Ohio, issued a warrant to search the Painesville residence and seize any evidence related to child exploitation (hereinafter this warrant shall be referred to as the “Residential Warrant”). During the January 22, 2016 residential search, agents seized a computer from Sullivan’s bedroom. In an interview conducted the same day by law enforcement, Sullivan admitted to accessing TOR on his computer, but he denied possessing or viewing any child

pornography on his computer. A subsequent search of defendant's computer revealed approximately 662 images and 145 videos of suspected child pornography.

On August 24, 2016, a two-count indictment was returned against Sullivan. Count 1 charges defendant with receipt and distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2). Count 2 charges Sullivan with possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). Defendant was arrested on these charges on August 31, 2016. During his transport to court to be processed and arraigned, and after being provided his *Miranda* warnings, Sullivan told an FBI agent, "I only looked at [TOR] one time."

II. LAW AND DISCUSSION

The key to this and other cases that have grappled with the constitutionality of the NIT Warrant was that Website A was located in the Eastern District of Virginia during the brief period it was operated by the FBI, but was communicating with computers that attempted to log onto the website from all over the country. As previously noted, defendant Sullivan's computer, for example, was physically located in Painesville, Ohio.

A. A Magistrate Judge's Authority to Issue Warrants

The Federal Magistrates Act provides that "[e]ach United States magistrate judge serving under [the Act] shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law" certain duties, including among other things "all powers and duties conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts[.]" 28 U.S.C. § 636(a)(1).

Rule 41(b) of the Federal Rules of Criminal Procedure addresses a federal magistrate judge's authority to issue warrants. Rule 41(b)(1) extends to a magistrate judge the authority to

issue warrants “to search for and seize” persons and property within the district in which she sits. The remaining provisions set forth specific instances wherein a magistrate judge may issue a warrant for persons and property that be located, or travel, outside her jurisdiction. Relevant to defendant’s suppression motion, Rule 41(b)(4) permits a magistrate judge to issue a warrant to install within the district a “tracking device” so that law enforcement can track the movement of persons and property within and outside the judicial district.

Additionally, Rule 41(b) was recently amended to add another exception to the requirement that the property to be searched and the persons to be seized be found in the magistrate judge’s district. Subsection 41(b)(6)(A), effective December 1, 2016, provides, in relevant part:

a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means

Defendant does not dispute that the NIT Warrant could have been properly issued under Rule 41(b)(6), had that provision been available to the Virginia magistrate judge on February 20, 2015. Sullivan further concedes, as he must, that any district court judge in the Eastern District of Virginia could have issued the warrant under the existing law in 2015.

B. Prior Decisions Addressing the NIT Warrant

Courts that have previously addressed the NIT Warrant have reached varying conclusions on the legal issues at play. Numerous courts have determined that the magistrate judge possessed adequate authority to issue the NIT Warrant under Rule 41(b), such that there was no legal violation that would require suppression. *See United States v. Lough*, No. 1:16-CR-18, 2016 WL 6834003 (N.D. W. Va. Nov. 18, 2016); *United States v. Johnson*, No. 15-CR-340 (W.D. Mo.

Oct. 20, 2016); *United States v. Smith*, No. 15-CR-467 (S.D. Tex. Sept. 28, 2016); *Jean*, 2016 WL 4771096; *United States v. Eure*, No. 2:16-CR-43, 2016 WL 4059663 (E.D. Va. July 28, 2016); *United States v. Matish*, No. 4:16-CR-16, 2016 WL 3545776 (E.D. Va. June 23, 2016); *Darby*, 2016 WL 3189703.

The vast majority of courts, including another judicial officer of this Court, have found that, while the NIT Warrant may have been issued unlawfully, suppression was not warranted, either under the exclusionary rule in general, or pursuant to the good faith exception set forth in *United States v. Leon*, 468 U.S. 897, 920, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984). See *United States v. Stepus*, No. 15-CR-30028, 2016 WL 6518427 (D. Mass. Oct. 28, 2016); *United States v. Allain*, No. 15-CR-10251, 2016 WL 5660452 (D. Mass. Sept. 29, 2016); *Libbey-Tipton*, No. 1:16-CR-236, Doc. No. 19 (N.D. Ohio Oct. 19, 2016); *United States v. Anzalone*, No. 15-CR-10347, 2016 WL 5339723 (D. Mass. Sept. 22, 2016); *United States v. Broy*, No. 16-CR-10030, 2016 WL 5172853 (C.D. Ill. Sept. 21, 2016); *United States v. Ammons*, No. 3:16-CR-11, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); *United States v. Knowles*, No. 2:15-CR-875, 2016 WL 6952109 (D. S.C. Sept. 14, 2016); *United States v. Scarbrough*, No. 3:16-CR-35, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016); *United States v. Henderson*, No. 16-CR-565, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Torres*, No. 5:16-CR-285, 2016 WL 4821223 (W.D. Tex. Sept. 9, 2016); *United States v. Adams*, No. 6:16-CR-11, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016); *United States v. Acevedo-Lemus*, No. 15-137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Rivera*, No. 2:15-CR-266-CJB-KWR (E.D. La. July 20, 2016); *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Epich*, No. 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Stamper*, No. 1:15-CR-109, 2016 WL 695660 (S.D. Ohio Feb.

19, 2016); *United States v. Michaud*, No. 3:15-CR-5351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

A small handful of courts have concluded that the NIT Warrant was unlawfully issued and suppressed all fruits of it. *See United States v. Croghan*, No. 1:15-CR-48, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); *United States v. Workman*, No. 15-CR-397-RBJ-I, 2016 WL 5791209 (D. Col. Sept. 6, 2016); *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016); *United States v. Arterbury*, No. 15-CR-182 (N.D. Ok. Apr. 25, 2016). Relying primarily on the decision from the District of Massachusetts, *Levin*, defendant urges the Court to join the minority of courts that have concluded that suppression of all evidence flowing from the execution of the NIT Warrant is necessary.

C. The NIT Warrant does not Violate Rule 41(b)

The government insists that case law dictates that Rule 41(b) is to be interpreted broadly. In support, it cites *United States v. N.Y. Tele. Co.*, 434 U.S. 159, 98 S. Ct. 364, 54 L. Ed. 2d 376 (1977), wherein the Supreme Court upheld a search warrant for a pen register to collect dialed telephone number information even though Rule 41 at the time did not specifically include electronic intrusions in the definition of property. In so holding, the Court observed that Rule 41 “is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause.” *Id.* at 169 & n.16. Then government also cites a more recent case where the Ninth Circuit Court of Appeals upheld a warrant allowing video surveillance, despite Rule 41's silence on this type of warrant. *See United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc), *opinion corrected* July 16, 1992. At a minimum, these cases suggest that Rule 41 is flexible enough to accommodate advancements in technology not envisioned when the rule

was promulgated.¹

The starting point for the Court’s analysis is Rule 41(b)(1), which permits a warrant for a search within the issuing magistrate judge’s district. The ending point is Rule 41(b)(4), which allows magistrate judges to issue warrants for “tracking devices” that are installed within the district. As an initial matter, defendant argues that Rule 41(b)(1) cannot apply because neither he, nor his computer, ever physically entered the Eastern District of Virginia. This may be true, but it is equally true that the agents monitoring Website A never physically left the Eastern District of Virginia. Still, a search took place. The Court must, therefore, determine where along the way the search took place, and this is where the Court believes Rule 41(b) must be flexible enough to recognize the technological advancements that have been ushered in courtesy of the Internet.

The Court finds persuasive guidance from courts that have determined that the search actually took place in Virginia. In *Darby*, the court reasoned that “[u]sers of [Website A] digitally touched down in the Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government

¹ The Court recognizes that some courts have rejected the notion that Rule 41(b) should be interpreted broadly. For example, in *Adams*, the court observed that neither *N.Y. Tele.* nor *Koyomejian* “authorize a magistrate judge to authorize a search of property outside his or her district pursuant to Rule 41(b)(1). This Court recognizes that some flexibility in the type of search is appropriate, but the Court is unwilling to expand the authority of the magistrate judge beyond the geographic limitations clearly established by Rule 41(b).” *Adams*, 2016 WL 4212079, at *5; *see also In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 570 (D. Md. 2011) (“*N.Y. Telephone Co.* expands the *type* of evidence of a crime for which a warrant may issue; it does not endorse issuance of a search warrant for the new and different purpose of obtaining information to aid in the apprehension of a criminal defendant.”) (internal citation omitted) (emphasis in original). The Court, however, does not understand the government to be advocating for the creation of additional exceptions to the geographic limitation placed on a magistrate judge’s authority to issue warrants. Rather, the government represents that the rule should be flexible enough to allow for virtual tracking; thus, going to the *type* of search permitted under the existing exceptions.

about their location.” *Darby*, 2016 WL 3189703, at *12. Other courts have similarly concluded that the activating computers digitally entered the Eastern District of Virginia when they logged into the website. *See Jean*, 2016 WL 4771096, at *15 (“whenever someone entered [Website A] he or she made a ‘virtual trip’ via the Internet to Virginia, just as a person logging into a foreign website containing child pornography makes a ‘virtual trip’ overseas”) (quoting *Matish*, 2016 WL 3545776, at *18).

Once a visitor entered Virginia by logging onto the website and downloading pornography, NIT was deployed and certain discrete identifying information was sent by the user’s computer. Thus, NIT operated as a virtual tracking device. One court explained the entire process as such:

[The defendant] took a virtual trip to the Eastern District of Virginia, but rather than travel by car, he traveled digitally—his vehicle was comprised of packets of information. Once there, the FBI attached a digital electronic tracking device to those packets, which [the defendant] virtually rode back to the Northern District of West Virginia. Upon his virtual return, [the defendant] parked his digital vehicle built of those packets of information on his computer, rather than in his driveway. At that point, the NIT sent back his digital address, just as a GPS tracker would send back his coordinates.

Lough, 2016 WL 6834003, at *6; *see Jean*, 2016 WL 4771096, at *15 (“the installation [of a tracking device by the FBI] did not occur on the government-controlled computer but on each individual computer that entered the Eastern District of Virginia when its user logged onto Playpen via the Tor network”). “When the computer left Virginia—when the user logged out of [Website A]—the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target’s location.” *Jean*, 2016 WL 4771096, at *15 (quoting *Matish*, 2016 WL 3545776, at *18).

Courts that have rejected the idea of a virtual tracking device have done so on the ground

that the NIT did not obtain the website user's IP address by tracking data but did so by searching the user's computer. *See Workman*, 2016 WL 5791209, at *4 ("The government did not obtain [defendant's] IP address by tracking the data as it moved through various relay nodes back to [defendant's] computer. Rather the government, through the NIT, searched [defendant's] computer and seized his IP address along with various other pieces of information."); *see also Adams*, 2016 WL 4212079, at *6 ("the NIT does not track; it searches"). Such an analysis fails to appreciate the realities that what is being tracked is the information as it travels from the website to the user's computer through the computer's code. That the information comes to rest with the user and his computer does not change the nature of tracking that takes place.² Like a traditional tracking device that sends back a location identifying signal, the NIT causes the computer to send back the location identifying information. "The fact that the NIT was purposely designed to allow the FBI to electronically trace the activating computer by causing it to return locating identifying information from outside the Eastern District of Virginia—is not only authorized by Rule 41(b)(4), but is the very purpose intended by the exception." *Jean*, 2016 WL 4771096, at *17.

However, defendant argues that the fact that Rule 41(b) has since been amended to specifically include a provision allowing for a warrant in situations where a suspect is using encryption software to conceal or mask his location is definitive evidence that the rule as it

² It is no different than a situation wherein a drug supplier ventures to the Eastern District of Virginia to obtain his shipment of drugs for subsequent distribution to various drug dealers, at which time law enforcement place a traditional physical tracking device on his vehicle. If the drug supplier returns to his home, parks his car in his driveway, and then has the individual drug dealers come to his house to receive their supply of drugs, one would not say that the device has ceased to be a tracking device merely because the vehicle to which it is attached ceases to move. Rather, it continues to send location information—albeit the same information—to the monitoring agents.

existed in 2015 could not support the NIT Warrant. He cites a May 4, 2014 letter from the Chair of the Advisory Committee on Criminal Rules to the Chair of the Committee on Rules of Practice and Procedure.³ Yet the letter's author merely emphasized the "special difficulties" the government faced investigating crimes involving electronic information and "anonymizing technologies," citing the fact that courts had reached different conclusions on whether warrants, like the NIT Warrant at issue here, could issue under the then-current language of Rule 41(b). The letter also addressed the complexities of crimes using multiple computers simultaneously as part of a complex scheme. The author does not state that Rule 41(b), at the time, was necessarily insufficient to handle these situations, only that there were different interpretations and that the rule should be updated to keep up with technological advancements. If anything, the letter serves to underscore the difficulty the digital age poses for judicial officers in the area of Fourth Amendment law. *See generally United States v. Gourde*, 440 F.3d 1065, 1074 (9th Cir. 2006) (in upholding district court's denial of a motion to suppress evidence of child pornography on defendant's computer, the court noted that "[w]e are acutely aware that the digital universe poses particular challenges with respect to the Fourth Amendment").

The Court finds that the NIT Warrant did not violate Rule 41(b). Defendant voluntarily and deliberately came to the Eastern District of Virginia when he took affirmative steps to log into the Playpen website by entering a username and password. (*See* NIT Warrant, Attachment A, at 216.) It is undisputed that the NIT software could not have been deployed if defendant had not made this virtual trip. *See Lough*, 2016 WL 6834003, at *6 ("the server did not reach out to him unsolicited") (citation omitted); *Jean*, 2016 WL 4771096, at *17 ("It is also undisputed that

³ Available at http://www.courts.gov/sites/default/files/fr_import/ST2014-05.pdf pp. 484-485.

but for Mr. Jean electronically traveling in search of child pornography to the watering hole in Virginia, the NIT could not have been deployed.”) (emphasis in original). Once in the district, the NIT was embedded in the material defendant was downloading and he carried it back to Ohio much like he would have carried a tracking device attached to his car. Once deployed, the NIT functioned in much the same way as a traditional tracking device sending location information back to the monitoring agents. The Court concludes that the language of Rule 41(b)(4) is flexible enough to support such an investigatory technique.⁴

D. Any Alleged Violation of Rule 41(b) Would not Require Suppression

In the end, the question of whether the NIT Warrant violated Rule 41(b) is academic, as the Court agrees with the vast majority of courts that have held that any alleged violation would not trigger the exclusionary rule. While the Fourth Amendment protects against unreasonable searches and seizures, it does not contain an enforcement mechanism. The exclusionary rule is a “judicial innovation,” *United States v. Clariot*, 655 F.3d 550, 553 (6th Cir. 2011), designed to

⁴ Defendant also argues that the NIT Warrant does not satisfy the particularity requirement because the warrant did not identify the computer in his Painesville, Ohio home as the place to be searched. (Mot. at 51-52.) The Fourth Amendment requires a warrant to “particularly describe[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “The purpose of this particularity requirement is to prevent the use of general warrants authorizing wide-ranging rummaging searches in violation of the Constitution’s proscription against unreasonable searches and seizures.” *United States v. Logan*, 250 F.3d 350, 365 (6th Cir. 2001) (citation omitted). The Court finds that the NIT Warrant was sufficiently particular. Attachment A of the NIT Warrant uses precise language to describe the place to be searched as the “activating computers” which are further described as “those [computers] of any user or administrator who logs into the [Website A] by entering a username and password.” (NIT Warrant, Attachment A, at 216.) Attachment B specifically describes the seven types of information that will be searched on each activating computer. (*Id.*, Attachment B, at 217.) The NIT Warrant does not suffer from a lack of particularity simply because “the warrant encompassed a large number of possible computers potentially located in a large number of districts; it merely indicates the FBI suspected a large number of users would access Website A from all over the country.” *Broy*, 2016 WL 5172853, at *3; *see Darby*, 2016 WL 3189703, at *8 (NIT Warrant sufficiently particular); *Acevedo-Lemus*, 2016 WL 4208436, at *7 n.4 (same); *Scarborough*, 2016 WL 5900152, at *14 (same); *Henderson*, 2016 WL 4549108, at *4 (same). Moreover, the fact that defendant’s use of the TOR software made it impossible to list his actual address (residential or IP) in the NIT Warrant does not render it a general warrant. *See Logan*, 250 F.3d at 365 (a “description contained in a warrant is sufficiently particular if it is as specific as the circumstances and the nature of the alleged crime permit”).

discourage the police from violating the Fourth Amendment. *Davis v. United States*, 564 U.S. 229, 236, 131 S. Ct. 2419, 180 L. Ed. 2d 285 (2011) (“The rule’s sole purpose . . . is to deter future Fourth Amendment violations.”) (collecting cases); see *United States v. Leon*, 468 U.S. 897, 916, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984); *United States v. Calandra*, 414 U.S. 338, 348, 94 S. Ct. 613, 38 L. Ed. 2d 561 (1974) (the exclusionary rule is a judicially created remedy which safeguards individual 4th Amendment rights by deterring police misconduct). It does not address the conduct of federal judges. See *Leon*, 468 U.S. at 916 (“To the extent that proponents of exclusion rely on its behavioral effects on judges and magistrates . . . their reliance is misplaced . . . the exclusionary rule is designed to deter police misconduct rather than punish the errors of judges and magistrates.”); *United States v. Master*, 614 F.3d 236, 242 (6th Cir. 2010) (The exclusionary rule is designed “to curb police rather than judicial misconduct.”) (quotation marks and citation omitted). The rule’s purpose is also not to remedy individual privacy violations. *Calandra*, 414 U.S. at 347 (“The purpose of the exclusionary rule is not to redress the injury to the privacy of the search victim[.]”); see *Davis*, 564 U.S. at 236 (citing, among authority, *Stone v. Powell*, 428 U.S. 465, 486, 96 S. Ct. 3037, 49 L. Ed. 2d 1067 (1976)).

Because operation of the rule carries the heavy societal cost of suppressing otherwise reliable evidence of unlawful behavior, it is not “an automatic consequence of a Fourth Amendment violation.” *Herring v. United States*, 555 U.S. 135, 136, 129 S. Ct. 695, 172 L. Ed. 2d 496 (2009); see *Davis*, 564 U.S. at 237 (noting that application of the rule “almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence” (citation omitted)); *Hudson v. Mich.*, 547 U.S. 586, 591, 126 S. Ct. 2159, 165 L. Ed. 2d 56 (2006) (noting that exclusion is a “last resort, not a first impulse”). Instead, in order for the exclusionary rule to

take root, “the deterrence benefits of suppression must outweigh its heavy costs.” *Davis*, 564 U.S. at 237 (citation omitted). Thus, operation of the exclusionary rule is limited “to situations in which [the purpose of deterring future Fourth Amendment violations] is ‘thought most efficaciously served.’” *Id.* at 237 (citation omitted). “Where suppression fails to yield ‘appreciable deterrence,’ exclusion is ‘clearly . . . unwarranted.’” *Id.* (quoting *United States v. Janis*, 428 U.S. 433, 454, 96 S. Ct. 3021, 49 L. Ed. 2d 1046 (1976)).

The good-faith exception to the exclusionary rule, first announced in *Leon*, recognizes the balance between enforcement of the Fourth Amendment and society’s interest in punishing criminal conduct. *See Davis*, 564 U.S. at 238-39. “The basic insight of the *Leon* line of cases is that the deterrence benefits of exclusion ‘var[y] with the culpability of the law enforcement conduct’ at issue.” *Id.* at 238 (quoting *Herring*, 555 U.S. at 143). Where “the police act with an objectively ‘reasonable good-faith belief’ that their conduct is lawful, or when their conduct involves only simple, ‘isolated’ negligence[,]” the high cost of suppression outweighs its deterrent benefit. *Id.* (quoting *Leon*, 468 U.S. at 909; *Herring*, 555 U.S. at 137). “[T]he crucial finding needed to suppress evidence is whether ‘police [mis]conduct [is] sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.’” *Master*, 614 F.3d at 243 (quoting *Herring*, 129 S. Ct. at 702).

Relying primarily upon the Massachusetts decision in *Levin*, defendant argues that the good-faith exception finds no application in the present case because the magistrate judge exceeded her jurisdiction, rendering the warrant void *ab initio*. (Mot. at 53 (citing, among authority, *Levin*, 186 F. Supp. 3d at 41.)) Defendant’s argument is foreclosed by the Sixth

Circuit's decision in *Masters*. There, a search warrant was issued by a state judge who lacked the authority to do so under state law (the judge sat in one county and the warrant was executed in another). Notwithstanding the fact that the warrant was void *ab initio*, the court ruled that in light of recent Supreme Court precedent, including *Herring*, the legal status of the warrant merely informed but did not control the good faith analysis. *Masters*, 614 F.3d at 243. The ruling in *Masters* was effectively at odds with an earlier Sixth Circuit decision in which the *Leon* good faith balancing test was rejected because the warrant in question had been issued by someone who lacked the legal authority to issue it. *Id.* at 241-42 (citing *United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001)). The court in *Masters* concluded, "[w]e do not believe, however, that such a broad interpretation of *Scott* continues to be viable in light of more recent Supreme Court cases." *Id.* at 242 (citing, among authority, *Herring*, *supra*). Courts within the Sixth Circuit, like *Ammons*, have held that the decision in *Masters* compels the conclusion that the *Leon* good faith analysis still applies, even if the NIT Warrant is void *ab initio*.⁵ *Ammons*, 2016 WL 4926438, at *8; *see also Scarbrough*, 2016 WL 5900152, at *1 (rejecting defendant's suggestion that it "reexamine" *Masters*, noting that "[t]his court does not 'reexamine' Sixth Circuit precedent. Instead, this court *follows* it.") (emphasis in original); *Libbey-Tipton*, No. 1:16-CR-236, Doc. No. 19 at *9-10 (relying on *Masters* to find that suppression was not appropriate).

Applying the balancing test required by Supreme Court and Sixth Circuit precedent, the

⁵ In reaching the conclusion that the good faith exception did not apply to the NIT Warrant, the court in *Levin* acknowledged the Sixth Circuit's decision in *Masters*, noting that the Sixth Circuit was one of the few appellate courts to reach the question of whether *Leon*'s good-faith exception applies when a warrant is void *ab initio*. In rejecting the analysis and conclusion of *Masters*, the court in *Levin* suggested that the Sixth Circuit interpreted "the Supreme Court's recent good-faith cases too broadly." *Levin*, 186 F. Supp. 3d at 40.

Court finds that, even if the magistrate judge exceeded her jurisdiction, suppression is not warranted because the record before this Court demonstrates that the FBI agents acted with good faith by diligently gathering information before submitting a detailed affidavit that fully apprised the issuing magistrate judge of all aspects of the NIT process, including the fact that the server for Website A would, at all times, be located in the Eastern District of Virginia, while the activating computers may be located outside the district. *See Ammons*, 2016 WL 4926438, at *9; *Werdene*, 2016 WL 3002376, at *16 (The FBI agents “provided the magistrate with all the information she needed to satisfy [herself] of [her] jurisdiction before proceeding.”) (quotation marks and citation omitted). At the hearing, defense counsel suggested that these seasoned agents should have realized that the magistrate judge lacked the authority to issue the NIT Warrant. However, given the varying treatment of the NIT Warrant by district courts and magistrate judges alike, “[t]he FBI agents can hardly be faulted for failing ‘to understand the intricacies of the jurisdiction of federal magistrates.’” *Ammons*, 2016 WL 4926438, at *16 (quoting *Darby*, 2016 WL 3189703, at *14); *Libbey-Tipton*, 1:16-CR-236, Doc. No. 19 at *12 (collecting cases); *see also* May 4, 2014 Advisory Committee Letter, *supra*. (noting the uneven treatment of such warrants by district courts).

The only possible benefit to be achieved by suppression, (again, assuming that the magistrate judge had acted without authority and violated Rule 41(b)), would be to deter future magistrate judges from making the same mistake. Yet, as of December 1, 2016, Rule 41(b) clearly and specifically provides for the very type of warrant that is at issue in this case. *See* Fed. R. Civ. P. 41(b)(6). Additionally, as previously observed, the exclusionary rule is directed to controlling the conduct of law enforcement and not the conduct of members of the judiciary. *See*,

e.g., *Broy*, 2016 WL 5172853, at *9 (noting both that the then-anticipated amendment to Rule 41 means that the deterrent effect on law enforcement would be “short lived,” and also underscoring the fact that the “exclusionary rule is designed to control the conduct of *law enforcement*, not the conduct of federal judges”)(citing *Leon*, 468 U.S. at 906-08) (emphasis in original). Suppression to punish or deter future magistrate judges would represent a misuse of the exclusionary rule. In the absence of any evidence that suppression would serve any legitimate deterrent effect on law enforcement, the good faith exception to the exclusionary rule would apply, and suppression would not be an appropriate remedy in this case.

III. CONCLUSION

For all of the foregoing reasons, defendant’s motion to suppress (Doc. No. 13) is denied.

IT IS SO ORDERED.

Dated: January 18, 2017



HONORABLE SARA LIOI
UNITED STATES DISTRICT JUDGE